Deutscher Bundestag **Drucksache 19/11330**

19. Wahlperiode 03.07.2019

Kleine Anfrage

der Abgeordneten Tobias Pflüger, Andrej Hunko, Michel Brandt, Christine Buchholz, Ulla Jelpke, Niema Movassat, Helin Evrim Sommer, Kathrin Vogler und der Fraktion DIE LINKE.

Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen

Im Jahr 2017 wurden verschiedene Dienststellen der Bundeswehr im Kommando Cyber- und Informationsraum (KdoCIR) zusammengelegt und mit dem Aufbau operativer Fähigkeiten begonnen (https://bit.ly/2Qj0wJ9). Das CERT (Computer-Emergency-Response-Team) der Bundeswehr (CERTBw) war bis dahin als defensive Einrichtung zum Schutz der IT-Netze der Bundeswehr bis zur Gründung des KdoCIR dem IT-Amt der Bundeswehr unterstellt und von der Gruppe Computer Netzwerk Operationen (CNO) im Kommando Strategische Aufklärung (KSA) getrennt. Mit der Aufstellung des KdoCIR wurden CERTBw und CNO den beiden neuen Dienststellen Zentrum Cyber-Operationen und Zentrum für Cyber-Sicherheit der Bundeswehr zugewiesen (https://bit.ly/2QwUGUQ). Das CERTBw hat bisher am CERT-Verbund mit Unternehmen, wissenschaftlichen Organisationen und zivilen Behörden teilgenommen und konnte sich so der Kompetenz und Erfahrung ziviler Akteure bedienen (www.cert-verbund.de/).

Während für den Schutz der Sicherheit und Vertraulichkeit von IT-Systemen nur mäßige Aufwüchse zu erkennen sind, baut die Bundesregierung im Bereich des Militärs und der Geheimdienste mit erheblichen finanziellen und personellen Ressourcen Strukturen auf, die aus Sicht der Fragestellerinnen und Fragesteller nicht mehr allein den Schutz vor bzw. die Abwehr von Cyberangriffen zur Aufgabe haben.

So wird von Vertretern der Bundesregierung und einschlägiger Stellen diskutiert, offensive Cyber-Operationen – sogenannte Hackbacks – in den Aufgabenkatalog aufzunehmen (z. B. hier: http://gleft.de/2Wo). Mit diesen offensiven Cyber-Operationen sind Eingriffe in Computersysteme in anderen Staaten gemeint, die aus Sicht der Fragestellerinnen und Fragesteller den Verpflichtungen aus internationalen Abkommen zuwider laufen und erhebliche sicherheitspolitische und militärische Risiken verursachen. Ein vom NATO Cooperative Cyber Defence Centre of Excellence berufenes Expertengremium hat im sog. Tallinn-Handbuch in einer Bewertung internationalen Rechts formuliert, dass Cyber-Angriffe, die von einem Staatsgebiet ausgehen und nicht unterbunden werden, einen Bruch internationalen Rechts darstellen (https://ccdcoe.org/research/tallinn-manual/). Werden diese von staatlichen Stellen verübt, können sie als Kriegshandlungen gewertet werden, die dem angegriffenen Staat die Rechtfertigung geben, gleichwertige Gegenmaßnahmen zu ergreifen – bei schweren Schäden auch in Form militärischer Aktionen (http://csef.ru/media/articles/3990/3990.pdf).

Die US-Administration hat in ihrer im September 2018 vorgelegten „National Cyber Strategy“ angekündigt, eine internationale Cyber-Abschreckungs-Initiative zu verfolgen und dafür gleichgesinnte Staaten in eine gemeinsame Abwehrstrategie einzubinden (vgl. https://bit.ly/2xrQ0XK).

Im Aachener Vertrag einigten sich die Bundesrepublik Deutschland und Frankreich auf die Zusammenarbeit im Bereich der Forschung und des digitalen Wandels, einschließlich der Themen Künstliche Intelligenz und Sprunginnovationen (vgl. Aachener Vertrag, Artikel 21, https://bit.ly/2IM1Lxf).

Wir fragen die Bundesregierung:

1. Kann die Bundesregierung Presseberichte bestätigen, wonach die meisten weltweiten Cyberangriffe im Jahr 2018 von Servern in den USA ausgingen und an zweiter Stelle die Niederlande und an dritter Stelle Deutschland stehen (http://gleft.de/2Wr)?
2. Falls die Bundesregierung von anderen Zahlen ausgeht, auf welche Quellen stützt sie sich dabei?
3. Was kann die Bundesregierung zum aktuellen Stand ihrer Überlegungen für eine „aktive Cyber-Abwehr“ mitteilen („Seehofer plant den Gegenangriff“, www.tagesschau.de vom 29. Mai 2019), und inwiefern betreffen diese auch die Bundeswehr und deren Kommando Cyber- und Informationsraum (KdoCIR)?
4. Inwiefern erwägt die Bundesregierung Hackbacks auch bei Angriffen, die von Systemen traditioneller Geheimdienste ausgehen?
5. Inwiefern erwägt die Bundesregierung Hackbacks auch bei Angriffen, die von Systemen befreundeter Geheimdienste ausgehen?
6. Inwiefern wäre ein Hackback durch deutsche militärische Stellen aus Sicht der Bundesregierung von der Budapest Convention on Cybercrime gedeckt, bzw. welche Änderungen wären diesbezüglich erforderlich?
7. Inwiefern war die Bundesregierung bezüglich einer internationalen Cyber-Abschreckungs-Initiative bereits in Kontakt mit US-Stellen, und unter welchen Rahmenbedingungen würde sie sich an einer solchen Initiative beteiligen?
8. In welchen Formaten hat sich die Bundesregierung an internationalen Gesprächsrunden, Verhandlungen oder Gremien
   a) zum Thema Cybersicherheit allgemein seit 2011 beteiligt (bitte nach Ressorts aufschlüsseln),
   b) zu Fragen der Abrüstung und Rüstungskontrolle in der Cyber-Kriegsführung seit 2011 beteiligt (bitte nach Ressorts aufschlüsseln)?
9. Schließt die Bundesregierung
   a) das Vorhandensein von Software-Implantaten anderer Staaten zum Monitoring von Computersystemen (vgl. https://nyti.ms/30BlFmK) in kritischen Infrastrukturen in Deutschland bzw.
   b) die Entwicklung oder Beschaffung vergleichbarer Software-Artefakte zur Verwendung in kritischen Infrastrukturen anderer Staaten aus?
10. Welche rechtlichen Studien, Einschätzungen und Bewertungen zieht die Bundesregierung für ihre Überlegungen zu Hackback-Maßnahmen und der damit einhergehenden Gefahr einer militärischen Eskalation heran?

11. Teilt die Bundesregierung die Sichtweise der in der Vorbemerkung der Fragesteller genannten NATO-Expertinnen und NATO-Experten, dass durch staatliche Stellen ausgeführte Cyberangriffe eine Form militärischer Angriffe darstellen können, und inwiefern berücksichtigt sie dies bei ihren Überlegungen zu Hackback-Maßnahmen?

12. Erwägt die Bundesregierung Mechanismen zur Bewertung von Eskalationsrisiken von Hackbacks und anderen Cyber-Operationen?

    a) Wenn ja, welche?

       Ist dabei auch eine politische Bewertungsinstanz vorgesehen?

    b) Wenn nein, weshalb nicht?

13. Legt die Bundesregierung Datensammlungen zur Analyse der Urheberschaft von Cyber-Angriffen an?

    a) Wenn ja, seit wann und auf welcher Rechtsgrundlage?

    b) Werden diese auch mit anderen Stellen der IT-Sicherheit ausgetauscht?

    c) Wenn ja, mit welchen?

    d) Plant die Bundesregierung die Anlegung von Datensammlungen und Zugängen zu Datenströmen zur Analyse der Urheberschaft von Cyber-Angriffen?

14. Inwiefern ist das CERT der Bundeswehr (CERTBw) von den operativen Teilen der Bundeswehr getrennt, bzw. wie wird diese Trennung aufgehoben?

15. Inwiefern wird das CERTBw nach Integration in das KdoCIR (https://bit.ly/2QwUGUQ) auch bei unklarer Trennung zwischen offensiven und defensiven Aufgaben im KdoCIR am zivilen CERT-Verbund teilnehmen können?

    Auf welche formale Handlungsgrundlage des CERT-Verbundes wird dabei Bezug genommen?

16. Inwiefern plant die Bundesregierung, ihre Erkenntnisse aus Cyber-Angriffen auch weiterhin mit dem zivilen CERT-Verbund zu teilen?

17. Welche personellen Ressourcen und Mittel erwägt die Bundesregierung für offensive Cyber-Operationen einzusetzen, und welche Einrichtungen und Kapazitäten bestehen diesbezüglich zum jetzigen Zeitpunkt (bitte nach Behörden bzw. GmbHs etc., z. B. BND – Bundesnachrichtendienst –, BfV – Bundesamt für Verfassungsschutz –, ZITIS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich –, KdoCIR, Agentur für Innovation in der Cybersicherheit, Bundespolizei aufschlüsseln)?

18. Welche Trainings oder „Cyber- Manöver“ haben das KdoCIR bzw. das Zentrum Cyber-Operationen (ZCO) seit deren Gründung mit privaten Firmen durchgeführt („Zentrum Cyber-Operationen kooperiert erfolgreich mit Firma CGI“, https://cir.bundeswehr.de ohne Datum), und in welchen dieser Veranstaltungen übernahm das ZCO die Rolle des „Red-Teams“?

19. An welchen Cyberübungen der Europäischen Union oder der NATO hat sich die Bundeswehr seit der Antwort der Bundesregierung auf Bundestagsdrucksache 19/1900 mit „Red-Teams“ beteiligt?

20. Welche Details kann die Bundesregierung zu der bilateralen Kooperation zwischen dem Allied Command Transformation (ACT) der NATO sowie dem Forschungsinstitut Center for Intelligence and Security Studies (CISS) an der Universität der Bundeswehr München (Schriftliche Frage 114 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/8434) mitteilen, und welche Projekte in den Bereichen strategische Vorausschau, Krisenfrüherkennung bzw. Krisenmonitoring „auch unter Rückgriff auf große Datenmengen“ sind dort geplant?

21. Inwiefern ist die konzeptionelle Prüfung der Einrichtung eines „Kompetenzzentrums Krisenfrüherkennung“ bei der Bundeswehr inzwischen abgeschlossen, und welche Details kann die Bundesregierung zu dessen Standort, Zielsetzung und technischer Infrastruktur mitteilen?

    Wer leitet das Zentrum?

22. Wann wird entschieden, ob das durch einen Lehrstuhlinhaber für Internationale Politik an der Universität der Bundeswehr München geleitete Pilotprojekt „Metis“ über die Dauer von zwei Jahren fortgeführt und demnach nicht am 1. Dezember 2019 endet (http://gleft.de/2WA), und inwiefern zeichnet sich bereits ab, dass das Projekt als erfolgreich oder erfolglos bewertet wird?

23. Welche Ergebnisse kann die Bundesregierung zu Prüfungen des Auswärtigen Amts mitteilen, für seine „strategischen Kommunikationsbedarfe“ die computergestützte Auswertung von sozialen Medien zum Erkennen von deutsche Außenpolitik betreffenden Desinformationen und Kampagnendynamiken in den sozialen Medien zu nutzen, und wie könnte dies technisch umgesetzt werden (Bundestagsdrucksache 19/7604, Antwort zu Frage 15)?

24. Wie will die Bundesregierung den geplanten EU-Ratsschlussfolgerungen nachkommen, wonach die Mitgliedstaaten „als Beitrag zu einem EU-weit gemeinsamen Verständnis der hybriden Bedrohungen auch künftig freiwillig Informationen und bewährte Verfahren“ austauschen sollen (Ratsdokument 9675/19), über welche Kanäle wird dies jetzt schon von der Bundesregierung umgesetzt, und inwiefern ist darin das Bundesministerium der Verteidigung eingebunden?

25. Inwiefern hat die Bundesregierung in Verhandlungen zur Etablierung des Rahmens „für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ („Cyberdiplomatischer Reaktionsrahmen“; Ratsdokument 9916/17 im Rahmen der „Cyber Diplomacy Toolbox“) dafür votiert, Listungen für Sanktion im Mehrheitsverfahren zu beschließen (vgl. Bundestagsdrucksache 19/10273, Frage 8; falls ja, bitte die Gründe darlegen)?

26. Enthält der EU-Rahmen zur Beantwortung böswilliger Cyberaktivitäten nach Auslegung der Bundesregierung auch Bestimmungen, die – nach Vorliegen rechtlicher Voraussetzungen – ein Eindringen der Bundeswehr in ausländische staatliche Informationssysteme und das Stören oder Abschalten derselben diplomatisch unterstützen kann?

27. Wie viele Mitarbeiterinnen und Mitarbeiter hat das Gemeinsame Lagezentrum Cyber- und Informationsraum (GLZ CIR) bei der Bundeswehr?

28. Welche Einstufung tragen die Lageberichte der nachgeordneten Bundeswehrdienststellen Kommando Strategische Aufklärung und Zentrum für Operative Kommunikation, die im Rahmen des Projekts „Lagebild für den Cyber- und Informationsraum“ als Datenquellen dienen (Bundestagsdrucksache 19/10391, Antwort zu Frage 3)?
    a) Welche Fachpublikationen werden hierfür ausgewertet, und wer sucht diese aus?
    b) Welche Einstufung trägt die aus den verschiedenen Datenquellen erstellte „Lage für den Cyber- und Informationsraum“, die auch an den Militärischen Abschirmdienst und das Nationale Cyber-Abwehrzentrum verteilt wird?
29. Welche Rolle haben die Cyber-Abwehr und damit verbundene Fragen in der Kooperation mit Frankreich und insbesondere im Rahmen des Aachener Vertrags gespielt, und inwiefern sind zukünftige gemeinsame Projekte dazu vorgesehen?
30. Mit welchen französischen Stellen hat sich die Bundesregierung entsprechend des Artikels 21 des Aachener Vertrags zur Frage ethischer Leitlinien für neue Technologien auf internationaler Ebene ausgetauscht, welche ethischen Fragestellungen und Probleme wurden dabei zugrunde gelegt, welche gemeinsamen Positionen wurden erarbeitet, und auf welchen internationalen Ebenen (UN, OSZE, Europarat, EU und andere) setzen sich Frankreich und Deutschland auf welche Weise für solche ethischen Leitlinien ein?

Berlin, den 24. Juni 2019

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333